Memory Forensics

Pattern-Oriented

Presented at VolgaCTF, Russia
Inter-Regional Inter-University Open Computer Security Contest
www.volgactf.ru

Dmitry Vostokov
Software Diagnostics Institute
Forensics

A discipline studying past structure and behavior.
Memory Forensics

A discipline studying past structure and behavior in acquired computer memory.
We Have A Problem

- Proliferation of computer architectures, operating systems, and tools
- Different memory analysis narratives
- Need to measure analysis quality
Solution

- Empirical patterns
- A pattern language
- Pattern orientation
Forensic Pattern

A common recurrent identifiable set of indicators (signs) together with a set of recommendations to apply in a specific context.
Memory Forensics revised

A discipline studying past structure and behavior of software in acquired memory using pattern-oriented analysis methodology.
Software Forensics

Software execution artefacts

Memory forensics
Software Forensics

A discipline studying past structure and behavior of software in execution artifacts using systemic and pattern-oriented analysis methodologies.
Structure and Behavior

- Memory snapshots (dumps)
- Traces and logs
- Source code
- Digital data (media)
Diagnostics and Forensics

- Diagnostics (present and past)
- Forensics (past)
- Prognostics (future)
Software Diagnostics

A discipline studying signs of software structure and behavior in software execution artifacts (such as memory dumps, software and network traces and logs) using systemic and pattern-oriented analysis methodologies.
Forensic Analysis Patterns

Software Diagnostics Patterns

Software Forensic Analysis Patterns

Memory Forensic Analysis Patterns

© 2014 Software Diagnostics Institute
A Pattern Language

- The same detection and analysis language for different computer architectures, operating systems, and tools
- The same memory analysis narratives
- Measured analysis quality
- Predicting unknown
Pattern Orientation

1. Pattern-driven
   - Finding patterns in memory
   - Using checklists and pattern catalogs

2. Pattern-based
   - Pattern catalogue evolution
   - Catalog packaging and delivery
Pattern Classification

... Dynamic Memory Corruption Patterns
Stack Overflow Patterns
Stack Trace Patterns
Symbol Patterns
Exception Patterns
Meta-Memory Dump Patterns
Module Patterns
Optimization Patterns
Thread Patterns
Process Patterns
...

© 2014 Software Diagnostics Institute
# Memory Acquisition Patterns

http://www.dumpanalysis.org/memory-acquisition-patterns

<table>
<thead>
<tr>
<th>Structural space patterns</th>
<th>Acquisition strategy patterns</th>
</tr>
</thead>
<tbody>
<tr>
<td>...</td>
<td></td>
</tr>
<tr>
<td>Process Memory Dump</td>
<td></td>
</tr>
<tr>
<td>Kernel memory Dump</td>
<td>External Dump</td>
</tr>
<tr>
<td>Physical Memory Dump</td>
<td>Self Dump</td>
</tr>
<tr>
<td>Fiber Bundle Dump</td>
<td>Conditional Dump</td>
</tr>
<tr>
<td></td>
<td>Dump Sequence</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
ADDR Patterns

http://www.dumpanalysis.org/addr-patterns

... 
Potential Functionality  Memory Copy 
Function Skeleton  Call Prologue 
Function Call  Call Parameter 
Call Path  Call Epilogue 
Local Variable  Call Result 
Static Variable  Control Path 
Pointer Dereference  Function Parameter 
Function Prologue  Structure Field 
Function Epilogue  Last Call 
Variable Initialization  ...

© 2014 Software Diagnostics Institute
Pattern Implementation

- By OS vendor (Windows, Mac OS X, Linux, …)
- By tool (WinDbg, Volatility, IDA, GDB, LLDB, …)
- By CPU architecture (x86, x64, ARM, …)
- By digital media (memory, volume, file, blob, …)
Pattern-Driven Analysis

Memory → Checklists ↔ Patterns → Action

✓ Pattern
✓ Pattern
✓ Pattern
✓ Pattern

2. Pattern catalogue checklists: [http://dumpanalysis.org](http://dumpanalysis.org)
Pattern-Based Analysis

Usage → Memory → Pattern Catalog + New Pattern → Discovery
Systems Approach

Narratology -> Trace Analysis Patterns -> Memory Analysis

© 2014 Software Diagnostics Institute
Native Memory Forensics

Using native OS debuggers such as WinDbg from Debugging Tools for Windows or GDB (Linux) or GDB/LLDB (Mac OS X).
Practical Examples

WinDbg session...
Patterns for Example A

- Tampered Dump
- Exception Stack Trace
- Stored Exception
- Lateral Damage
- Execution Residue
- Hidden Exception
- NULL Data Pointer
Patterns for Example B

- Heap Corruption
- Stack Trace Collection
- RIP Stack Trace
- Hooksware
- Patched Code
- Hidden Module
- Deviant Module
- String Hint
- Fake Module
- No Component Symbols
- Namespace
Example C

Pattern correspondence

- Process Dump
- Physical (Complete) Dump
- Kernel Dump
Further Reading (Patterns)

- The Timeless Way of Building (by Christopher Alexander)
- A Pattern Language: Towns, Buildings, Construction (by Christopher Alexander, et al.)
Further Reading (MDA)

- Cloud Memory Dump Analysis
- Fundamentals of Physical Memory Analysis
- Victimware
- Pattern-Oriented Software Forensics
- Debugging TV
Further Reading (SD)

- Software Diagnostics Institute
- Pattern-Driven Software Diagnostics
- Systemic Software Diagnostics
- Pattern-Based Software Diagnostics
- Philosophy of Software Diagnostics
Current Reference

Memory Dump Analysis Anthology: 7 volumes + 3 colour volumes

Volume 8 is planned for 2015/2016
Forthcoming Transcript

Pattern-Oriented Memory Forensics: A Pattern Language Approach
(ISBN: 9781908043764)
A Pattern Language for Software Diagnostics, Forensics, and Prognostics: Memory, Traces, Deconstruction (10 volumes)
Q&A

Please send your feedback using the contact form on DumpAnalysis.org
Thank you for attendance!